B u c h r e z e n s i o n

Dieter Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. C.H. Beck, München 2015, 691 S., € 89,-.

Man durfte gespannt sein auf das Buch von *Dieter Kochheim*, der nicht nur ein ausgewiesener Kenner der Materie Cybercrime ist, sondern sich auch als Betreiber der Webseite www.cyberfahnder.de einen Namen gemacht und auf dessen Expertise schon so mancher online zugegriffen hat. Nun ein haptisches Werk in den Händen zu halten, erleichtert nicht nur das kurze Nachschlagen, sondern vereint Geschichte, Technik, materielles und prozessuales Recht rund um das Thema Cybercrime in einem Band.

Der erste Teil „Duale Welt" gibt zunächst einen inhaltlichen Überblick über die Themen des Gesamtwerkes, um dann im 1. Kapitel eine Begriffsklärung von Cybercrime und IuK-Strafrecht im engeren und weiteren Sinne sowie organisierten Formen von Cybercrime vorzunehmen (S. 13 f.). Anschließend wird der Begriff des informationstechnischen Systems, wie ihn das BVerfG in seiner Entscheidung zur Onlinedurchsuchung prägte, näher präzisiert und in einen technischen Kontext gestellt. Hilfreich ist in diesem Zusammenhang die Auflistung der technischen Systeme in ihrer Dimensionierung und Qualifizierung als informationstechnische Systeme (S. 17). Einführend werden zudem die wichtigsten Tatbestände des IuK-Strafrechts vorgestellt und in Tabellenform ein Überblick über den Strafrahmen gegeben (S. 23). Neben statistischen Fallzahlen und kriminalpolitischer Bedeutung (S. 25 ff.), benennt *Kochheim* die zehn vom BSI 2012 beschriebenen Bedrohungen gegen Anlagensteuerungen (S. 30 ff.).

Sehr interessant ist dann auch der historische Abriss zum Thema Cybercrime in Kapitel 2 (S. 33 ff.). Die technische Entwicklung von den Lochstreifen aus Holzplättchen für Webstühle 1728 bis zur Kreditkarte 1894 wird kurz nachgezeichnet. Danach wird im Zeitraffer die Geschichte der Elektrotechnik bis 1950, das elektronische Zeitalter bis 1970, die elektronische Gründerzeit bis 1980 und Expansion und Missbrauch bis 1990 beschrieben. Umfangreich gestaltet sich dann der historische Abschnitt bis 2000, da nun die IT den Massenmarkt eroberte, das Internet zum Massenmedium wurde und sich das Cybercrime zu organisieren begann (S. 45). Mit Blick auf die Zeit ab 2000 („Kommerzielles Internet und organisiertes Cybercrime") werden neu beginnende Phänomene wie die Entwicklung von Malware, Botnetzen u.ä. beschrieben (S. 66 ff.). Es folgt die differenzierte Betrachtung neuer Formen des Cybercrimes in der Neuzeit (S. 73 ff.). Hier erfährt man etwas darüber, was Cardingboards, Botnetze oder das Stuxnet sind, lernt unterschiedliche Formen der Datenspionage, wie etwa die bekannten Man-in-the-Middle-Attacken aber auch unbekanntere wie Night Dragon oder Operation High Roller kennen und erhält einen kurzen Input zu Ransomware, Abofallen und Betrügereien in Webshops.

Kapitel 3 (S. 91 ff.) beschäftigt sich ausführlich mit den Formen und Methoden des Cybercrimes und zeigt die technische Seite der Materie auf, was sich als sehr hilfreicher Hintergrund für die spätere rechtliche Betrachtung erweist. Schaubilder erleichtern es hier – wie auch schon an anderer Stelle – dem Leser eine Vorstellung von den doch recht komplexen Vorgängen zu vermitteln. So werden beispielsweise Hacking, Phishing, Skimming und Angriffe mit Malware umfassend, in ihren Differenzierungen und detailgenau erläutert. Abschließend wird auf Identitätstäuschung und Identitätsdiebstahl sowie kurz auf Carding und Kontobetrug eingegangen.

In Kapitel 4 (S. 131 ff.) folgt unter der Überschrift „Gefahren und Hakteure in der dualen Welt" eine Betrachtung der für das Cybercrime bedeutenden gesellschaftlichen und strukturellen Umgebungen.

Der zweite Teil des Buches, der zugleich der umfangreichste Teil ist, stellt den zentralen Abschnitt des Werkes dar und beleuchtet das materielle IuK-Strafrecht in seinen verschiedenen Facetten (S. 151 ff.). Dabei werden nicht nur die einschlägigen Straftatbestände im Detail vorgestellt und in einen Zusammenhang mit den technischen Besonderheiten gestellt, sondern auch voll umfänglich die einschlägige Rechtsprechung wiedergegeben und bei der Bewertung berücksichtigt.

Zunächst wird in Kapitel 5 das Hacking umfassend dargestellt und mit einer Abgrenzung nach Gegenstand und Grenzen des Hacking-Strafrechts begonnen (S. 154 ff.). Einen guten Überblick erhält man durch eine tabellarische Übersicht, in der nach Strafbarkeiten des klassischen Hackings, Straftatbeständen zum Abhörschutz, zum Schutz des Rechtsverkehrs, strafbaren Vorbereitungshandlungen und Verbrechensverabredung differenziert wird (S. 160 ff.). Es folgt eine ausführliche Betrachtung dieser Straftatbestände im Einzelnen, wobei es dem *Autor* wiederum durch Angriffsszenarien veranschaulichende Grafiken gelingt, das Verständnis dieser doch komplizierten Technikseite der Straftatbestände zu erleichtern. Auch eine Grafik zu den verschiedenen Tatphasen ist sehr hilfreich.

Kapitel 6 beschäftigt sich mit der Verbreitung und dem Einsatz von Basis-Malware, wobei eine Differenzierung nach den einzelnen Phasen erfolgt und auch hier Grafiken das Bild abrunden (S. 209 ff.). In Kapitel 7 wird kurz auf die Strafbarkeit bei Betrieb und Steuerung eines Botnetzes eingegangen und die Verbrechenstatbestände benannt, die bei spezialisierter Botware gegen kritische Infrastrukturen in Betracht kommen können (S. 239 ff.). Ebenfalls recht kurz erfolgt die Darstellung der missbräuchlichen Datenverwertung und Rechtsverfolgung in Kapitel 8 (S. 245 ff.), wobei auch schon auf den neuen Straftatbestand gegen die Datenhehlerei eingegangen wird (S. 253 f.), der nach Erscheinen dieses Buches mittlerweile in Kraft getreten ist. Kapitel 9 beschäftigt sich mit dem bargeldlosen Zahlungsverkehr, seinen technischen und wirtschaftlichen Abläufen sowie den grundlegenden Rechtsfragen (S. 255 ff.). Auch hier erleichtern Grafiken das Verständnis für die unterschiedlichen Abbuchungsverfahren und Rechtsstrukturen. Neben klassischen Verfahren werden die neuen Zahlungsverfahren beschrieben, die ebenfalls Missbrauchsgefahren bergen (S. 281).

Kapitel 10 beleuchtet betrugsnahe Erscheinungsformen des Cybercrimes, wie betrügerische Webshops, Abofallen, Kartenmissbrauch, Manipulationen mit Bankkonten u.ä. (S. 283 ff.). In Kapitel 11 werden die Erscheinungsformen beim Missbrauch von Zahlungsmitteln, des Zahlungs- und Warenverkehrs behandelt, wobei auch hier zunächst eine Tabelle zur Orientierung bei den verschiedenen Formen des Cybercrimes dient, die in Verbindung mit Bezahlsystemen und dem Warenhandel stehen (S. 309 ff.). Die verschiedenen Phasen und Strafbarkeiten, die das mehrgliedrige Delikt des Skimmings verwirklicht, werden in Kapitel 12 beschrieben (S. 321 ff.). Auch hier gibt eine Tabelle mit den Fälschungsdelikten einen Überblick (S. 325), Grafiken zu Tatphasenmodellen beim Skimming erleichtern wieder das Verständnis (S. 330, 335, 338). Kapitel 13 behandelt die Identitätstäuschung und den Identitätsdiebstahl unter dem Gesichtspunkt des Urkundenstrafrechts (S. 356 ff.). Eine Tabelle beschreibt am Ende überblicksartig, welche strafrechtlichen Konsequenzen die Namens- und Identitätstäuschung bei der Einrichtung und Nutzung von Webkonten, bei digitaler Kommunikation, Anlagen und gehosteten Dateien sowie technischen Manipulationen haben kann (S. 385 ff.). Viel Raum wird auch den verschiedenen Phasen des Phishings in Kapitel 14 gewidmet (S. 395 ff.). Festgestellt wird hier, dass alle Phasen der zentralen Handlung beim Phishing, nämlich die Kontomanipulation, einen Computerbetrug in Tateinheit mit dem Fälschen beweiserheblicher Daten verwirklichen (S. 418). Im Kapitel werden aber auch die anderen Handlungen und Phasen des Phishings einer strafrechtlichen Bewertung zugeführt und Sonderformen wie beispielsweise das Pharming beschrieben und der strafrechtliche Rahmen abgesteckt. Kapitel 15 beschäftigt sich mit dem Onlinehandel und der Underground Economy (S. 423 ff.). Hier erfährt der Leser nicht nur, welche illegalen Handelsgeschäfte im Internet betrieben werden und welche strafrechtlichen Werbeverbote tangiert sein können (Tabelle auf S. 425 f.), sondern es werden auch die unterschiedlichen Handlungsmodelle für Abofallen dargestellt und unter Berücksichtigung der einschlägigen Rechtsprechung einer rechtlichen Bewertung zugeführt. Auch hier finden sich veranschaulichende Grafiken. Ebenfalls beschrieben und nach strafrechtlichen Gesichtspunkten konkretisiert werden z.B. Carding- und andere Boards, in denen kriminelle Geschäfte angebahnt und abgewickelt werden können. Auch Bullet Proof-Dienste und Anonymisierungsdienste werden technisch skizziert, die Anonymisierungsmöglichkeiten grafisch dargestellt und auf die Schwierigkeiten hingewiesen, diesbezüglich eine Strafbarkeit zu begründen (z.B. S. 449). Abgerundet wird das Kapitel durch einen kurzen Input zu den Schwierigkeiten, aufgrund der neuen Instrumente im Zahlungsverkehr die Zahlungsströme zu verfolgen und somit den Straftatbestand der Geldwäsche zu belegen. Hier merkt *Kochheim* kritisch an: „Die streckenweise hilflos wirkenden Ausführungen in diesem Abschnitt beruhen darauf, dass der Gesetzgeber weder die Betreiber krimineller Boards, von Bullet-Proof-Diensten noch von Strukturen für die Verschleierung von Zahlungsströmen und zur Beutesicherung vor Augen hatte, als er die Vorschriften zum IuK-Strafrecht und zur Geldwäsche schuf“ (S. 461). Eine kriminalpolitische Forderung nach mehr Strafrecht in diesem Bereich wird aber nicht angeschlossen, vielmehr lediglich auch auf die praktischen Probleme bei der Strafverfolgung hingewiesen.

Abgeschlossen wird der zweite Teil durch Kapitel 16 zu den Äußerungsdelikten (S. 463 ff.) und Kapitel 17 zu pornographischen Abbildungen (S. 469 ff.). Auch bei diesen Themengebieten geben jeweils Tabellen einen Überblick darüber, welche Straftatbestände im Einzelnen verwirklicht werden können.

Teil 3 befasst sich auf knapp 100 Seiten mit den strafprozessualen Besonderheiten im Zusammenhang mit dem Cybercrime (S. 479 ff.). Eingeführt wird mit einem „Allgemeinen Teil der Auseinandersetzung mit der Strafverfolgung“ (S. 481), der grundsätzliche Ausführungen zu den Aufgaben der Strafverfolgung, Ermittlungshandlungen, Verdachtsmomenten und Verwertungsgrenzen und -verboten macht. Abgerundet wird dieses Kapitel 18 mit einem tabellarischen Überblick über die einzelnen Ermittlungsmaßnahmen (S. 514 ff.). Kapitel 19 wird dann spezieller und behandelt das Internet und die IuK-Technik als Informationsquellen (S. 519 ff.). Einleitend wird die wichtige Entscheidung des BVerfG zur Onlinedurchsuchung wiedergegeben und danach der Rahmen des Persönlichkeitsschutzes durch die Grundrechte abgesteckt. Sodann wird auf das Massenproblem im Zusammenhang mit dem Gebot der vollständigen Dokumentation aller Ermittlungshandlungen hingewiesen. Als Lösung benennt *Kochheim* die konsequente Beschränkung der Spurenerhebung (S. 531). In Kapitel 20 werden Informationsquellen und Sachbeweise beschrieben (S. 533 ff.) und zunächst mit öffentlichen Quellen und behördlichen Auskünften begonnen. Danach wird bei Auskünften von Privatleuten und Firmen nach Bestandsdaten und Verkehrsdaten differenziert und es werden die einschlägigen Ermächtigungsnormen benannt. Bei der Durchsuchung wird nach Durchsicht und Sicherung vor Ort und Ferndurchsicht differenziert. Etwas kurz kommt hierbei die umstrittene Frage, inwieweit ein Zugriff auf ausländische Cloud-Speicher durch Ermittlungsbehörden möglich ist oder nicht (S. 547). Ausführlicher wird dagegen bei der Beschlagnahme von E-Mail-Konten differenziert und auf die unterschiedliche Rechtsprechung von BVerfG und BGH hingewiesen. *Kochheim* konstatiert, dass die von beiden Gerichten geforderte Auswertung der Daten rechtliche Schwierigkeiten bereite (S. 550).

Kapitel 21 beschäftigt sich mit personellen Ermittlungen (S. 551 ff.), wobei zunächst Informanten von Vertrauenspersonen abgegrenzt werden. Es folgt eine Beschreibung von nicht offen ermittelnden Beamten und verdeckten Ermittlern sowie eine Ausführung der einschlägigen Vorschriften in RiStBV und StPO. Danach werden diese Grundsätze auf das Internet übertragen und nach allgemeiner Internet-Patrouille, Verwendung einer einfachen Legende und Überwindung besonderer persönlicher Schutzvorrichtungen differenziert (S. 560 f.). Schließlich wird den rechtlichen Rahmenbedingungen für die Nutzung fremder Zugangsdaten, Keuschheitsproben und Scheinkauf von Ermittlungsbeamten nachgegangen. Abgeschlossen wird Teil 3 durch die kurze Darstellung der technischen Maßnahmen in Kapitel 22 (S. 565 ff.). Hier finden sich sehr knappe rechtliche Anmerkungen zur Obser-

vation durch technische Mittel, Überwachung der Telekommunikation, Auslandsüberwachung, IMSI-Catcher, Onlinedurchsuchung, Quellen-TKÜ, Spyware und Crawler.

Komplettiert wird das Buch durch ein 75-seitiges Glossar (S. 575 ff.), das es dem Leser ermöglicht, schnell beim Lesen Fachtermini nachzuschlagen und so kurz und verständlich eine Begriffsklärung zu erhalten. Auch dies erleichtert, neben dem umfangreichen Grafik- und Tabellenmaterial, den Umgang mit der komplexen Materie.

Cybercrime in allen seinen Facetten würde ganze Bücherregale füllen, hier hält man ein Buch in den Händen, das – gerade im materiell-rechtlichen Teil – keine Wünsche offen lässt und anhand von Streifzügen durch Geschichte und Technik das Gesamtverständnis des Lesers erheblich erhellt. Der strafprozessuale Teil ist dagegen ein wenig knapp ausgefallen – einen guten Überblick liefert aber auch er. Angesichts der geringen Halbwertzeit von Gerichtsentscheidungen und Rechtslage rund um das große Thema Cybercrime bleibt zu hoffen, dass *Kochheim* nicht nur sein Online-Portal gewohnt aktuell hält, sondern der Beck-Verlag auch in regelmäßigem Turnus diesen Band neu auflegt.

Prof. Dr. Anja Schiemann, Münster